

- [1] A. Languasco and A. Perelli. On Linnik's theorem on Goldbach numbers in short intervals and related problems. *Ann. Inst. Fourier*, 44:307–322, 1994. http://archive.numdam.org/article/AIF_1994__44_2_307_0.pdf, MR1296733 (95g:11097).

Abstract: Linnik proved, assuming the Riemann Hypothesis, that for any $\varepsilon > 0$, the interval $[N, N + \log^{3+\varepsilon}N]$ contains a number which is the sum of two primes, provided that N is sufficiently large. This has subsequently been improved to the same assertion being valid for the smaller gap $C \log^2 N$, the added new ingredient being Selberg's estimate for the mean-square of primes in short intervals. Here we give another proof of this sharper result which avoids the use of Selberg's estimate and is therefore more in the spirit of Linnik's original approach. We also improve an unconditional result of Lavrik's on truncated forms of Parseval's identity for exponential sums over primes.

- [2] A. Languasco. Some results on Goldbach's problem. *Rend. Sem. Mat. Univ. Politec. Torino*, 53(4):325–337, 1995. <http://seminariomatematico.dm.unito.it/rendiconti/cartaceo/53-4/325.pdf>, MR1452389 (98f:11106).

Abstract: In Section 1 we introduce the Goldbach Conjecture and give a brief account on the main contribution to this subject. In the other sections we sketch the proofs of some results on the existence of Goldbach numbers in short intervals and on the exceptional set for Goldbach's problem.

- [3] A. Languasco and A. Perelli. A pair correlation hypothesis and the exceptional set in Goldbach's problem. *Mathematika*, 43:349–361, 1996. <http://dx.doi.org/10.1112/S0025579300011827>, MR1433280 (98g:11113).

Abstract: Let

$$E(X, H) = |\{2n \in [X, X + H] : 2n \text{ is not a sum of two primes}\}|$$

be the exceptional set for Goldbach's problem in short intervals. We will assume the Generalized Riemann Hypothesis and that, for $(a, q) = 1$, $\varepsilon > 0$ and $\theta \in (0, \frac{1}{2}]$ fixed,

$$F(X, T; q, a) = \sum_{\chi_1, \chi_2 \pmod{q}} \chi_1(a) \bar{\chi}_2(a) \tau(\bar{\chi}_1) \tau(\chi_2) \sum_{|\gamma_1|, |\gamma_2| \leq T} X^{i(\gamma_1 - \gamma_2)} w(\gamma_1 - \gamma_2) \ll q^2 T X^\varepsilon,$$

where $w(u) = \frac{4}{4+u^2}$, $\tau(\chi)$ denotes the Gauss sum and γ_j , $j = 1, 2$, run over the imaginary part of the non trivial zeros of $L(s, \chi_j)$, holds uniformly for $\frac{X^{1-\theta}}{q} \leq T \leq X$ and $q \leq X^\theta$. Under the previous hypotheses we prove, for every $\varepsilon > 0$ fixed, that

$$E(X, X^{2\theta}) \ll_\varepsilon X^\varepsilon,$$

i.e. for $\theta > \frac{\varepsilon}{2}$ all even integers in any interval of the form $[X, X + X^{2\theta}]$ but $O(X^\varepsilon)$ exceptions are a sum of two primes.

- [4] A. Languasco. A note on primes and Goldbach numbers in short intervals. *Acta Math. Hungar.*, 79:191–206, 1998. <http://dx.doi.org/10.1023/A:1006553707162>, MR1616038 (99g:11104).

Abstract: Let $J(N, H)$ be the Selberg integral and $E(x, T)$ the error term in Kaczorowski-Perelli's weighted form of the classical explicit formula. We prove that the estimate $J(N, H) = o(H^2 N)$ is connected with an appropriate estimate of $\int_N^{2N} |E(x, T)|^2 dx$, uniformly for H and T in some ranges. Moreover, assuming a suitable bound for the quantity $\int_N^{2N} |E(x, T)|^2 dx$, we also obtain, for all sufficiently large N and $H \gg (\log N)^{11/2}$, that every interval $[N, N + H]$ contains $\gg H$ Goldbach numbers.

- [5] A. Languasco. A singular series average and Goldbach numbers in short intervals. *Acta Arith.*, 83:171–179, 1998. <http://matwbn.icm.edu.pl/ksiazki/aa/aa83/aa8321.pdf>, MR1490647 (98k:11139b).

Abstract: Let $\mathfrak{S}(n) = 2 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{\substack{p|n \\ p>2}} \left(\frac{p-1}{p-2}\right)$ if n is even and $\mathfrak{S}(n) = 0$ if n is odd, be the singular series of the Goldbach problem. Let $\nu \geq 1$ be a fixed real number. We prove that

$$\sum_{n \leq X} \mathfrak{S}(n)^\nu = c_1 X + c_2 (\log X)^\nu + O((\log X)^{\nu-1/3}),$$

where c_1, c_2 and the implicit constant depend on ν . As a consequence, we improve the known results on the positive proportion of Goldbach numbers in short intervals.

- [6] A. Languasco. A conditional result on Goldbach numbers in short intervals. *Acta Arith.*, 83:93–103, 1998. <http://matwbn.icm.edu.pl/ksiazki/aa/aa83/aa8327.pdf>, MR1490641 (98k:11139a).

Abstract: Assume the Riemann Hypothesis and a weaker form of Montgomery’s pair correlation conjecture, i.e., for every $\theta \in [1, 2)$

$$F(X, T) = 4 \sum_{0 < \gamma_1, \gamma_2 \leq T} \frac{X^{i(\gamma_1 - \gamma_2)}}{4 + (\gamma_1 - \gamma_2)^2} \ll T(\log T)^\theta,$$

where γ_j , $j = 1, 2$, run over the imaginary part of the non-trivial zeros of the Riemann zeta-function, holds uniformly for $\frac{X}{H} \leq T \leq X$, where $1 \leq H \leq X$. Then, for all sufficiently large X and $H \gg (\log X)^\theta$, we have that the interval $[X, X + H]$ contains a even integer which is a sum of two primes.

- [7] A. Languasco. Some refinements of error terms estimates for certain additive problems with primes. *J. Number Theory*, 81:149–161, 2000. <http://dx.doi.org/10.1006/jnth.1999.2468>.

Abstract: We study, under the assumption of the Generalized Riemann Hypothesis, the individual and mean-square error terms for the number of integers representable as a sum of $k \geq 3$ primes. We improve, using a smoothing technique, Friedlander-Goldston’s recent results on this topic. Moreover, we remark that the argument we use can also be applied to other similar problems.

- [8] A. Languasco. An Introduction to Cryptography. *Queen’s Papers in Pure and Applied Mathematics*, 119(121-140), 2000. in “The Curves Seminar at Queen’s”, vol. 13, ed. da A.V. Geramita.

Abstract: In this introduction to Cryptography, we start by giving some basic notions from elementary number theory and see how they can be applied to send “secret” messages. After introducing congruence theory, Fermat’s little theorem and the Euler-Fermat theorem, we examine, from a historical point of view, some classic cryptographic systems. Then we give the main properties of modern cryptographic systems and, in particular, we define public key cryptography. One of the most important public-key systems (which exploits the fact that in \mathbb{Z} primality algorithms are much “faster” than factorization ones) is presented: the R.S.A. cryptosystem. We also present another public key system which exploits the discrete logarithm problem and which is also consistently used as an alternative to R.S.A. (for example the U.S. government offices use it for their digital signature scheme). An analogue of the discrete logarithm problem is used in the so-called “elliptic curves cryptosystems”. Unfortunately, the amount of mathematical theory needed to understand the elliptic curves method is too great to be explained here. So, we will say, in the last paragraph, just a few words on the differences between the discrete logarithm problem and its elliptic curve analogue. This article is geared toward the amateur interested in the subject.

- [9] D. Bazzanella and A. Languasco. On the asymptotic formula for Goldbach numbers in short intervals. *Studia Sci. Math. Hungar.*, 36:185–199, 2000. <http://dx.doi.org/10.1556/SScMath.36.2000.1-2.14>, MR1768230 (2001j:11096).

Abstract: Let $R(k) = \sum_{l+m=k} \Lambda(l)\Lambda(m)$, $\mathfrak{S}(k) = 2 \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{\substack{p|k \\ p>2}} \left(\frac{p-1}{p-2}\right)$ if k is even and $\mathfrak{S}(k) = 0$

if k is odd. It is known that $R(k) \sim k\mathfrak{S}(k)$ as $N \rightarrow \infty$ for almost all $k \in [N, 2N]$ and that

$$\sum_{k \in [n, n+H]} R(k) \sim \sum_{k \in [n, n+H]} k\mathfrak{S}(k) \quad \text{for } n \rightarrow \infty \quad (1)$$

uniformly for $H \geq n^{1/6+\epsilon}$. Here we prove, assuming $N^\epsilon \leq H \leq N^{1/6+\epsilon}$ and $N \rightarrow \infty$, that (1) holds for almost all $n \in [N, 2N]$.

- [10] J. Kaczorowski, A. Languasco, and A. Perelli. A note on Landau’s formula. *Funct. Approx. Comment. Math.*, 28:173–186, 2000. Dedicated to Włodzimierz Staś on the occasion of his 75th birthday. <http://www.staff.amu.edu.pl/~fa/XXVIII/fa-28-1-173.pdf>, MR1824002 (2001m:11156).

Abstract: Landau proved, for any fixed $x > 1$, that

$$\sum_{0 < \gamma \leq T} x^\rho = -\frac{T}{2\pi} \Lambda(x) + O(\log T) \quad \text{for } T \rightarrow \infty,$$

where ρ runs over the non-trivial zeros of the Riemann zeta function $\zeta(s)$ and $\Lambda(x) = \log p$ if $x = p^m$, p prime and $\Lambda(x) = 0$ otherwise. Recently Gonek has obtained a form of the previous formula which is uniform in T and x . Here we furnish a uniform version of Landau’s formula in which the error term has sharper individual and mean-square estimates.

- [11] A. Languasco and A. Perelli. Pair correlation of zeros, primes in short intervals and exponential sums over primes. *J. Number Theory*, 84(2):292–304, 2000. <http://dx.doi.org/10.1006/jnth.2000.2511>, MR1796516 (2001m:11151).

Abstract: Assume the Riemann Hypothesis and let $F(X, T) = 4 \sum_{0 < \gamma_1, \gamma_2 \leq T} \frac{X^{i(\gamma_1 - \gamma_2)}}{4 + (\gamma_1 - \gamma_2)^2}$, where γ_j , $j = 1, 2$, run over the imaginary part of the non-trivial zeros of the Riemann zeta-function, be the Montgomery's pair correlation function. Goldston-Montgomery proved, for any $\epsilon > 0$, that $F(X, T) \sim \frac{1}{2\pi} T \log T$ uniformly for $X^\epsilon \leq T \leq X$ is equivalent to $J(X, H) \sim HX \log \frac{X}{H}$ uniformly for $1 \leq H \leq X^{1-\epsilon}$ where $J(X, H)$ is Selberg's integral. Here we prove, for any $\epsilon > 0$, that $F(X, T) \sim \frac{1}{2\pi} T \log T$ uniformly for $X^{1/2+\epsilon} \leq T \leq X$ is equivalent to a suitable asymptotic formula for the truncated mean-square of exponential sums over primes.

- [12] A. Languasco and A. Perelli. Numeri Primi e Crittografia. In M. Emmer, editor, *Matematica e Cultura 2000*, pages 227–233, Venezia, 2000. Springer-Verlag, Milano. trad. inglese in *Mathematics and Culture I*, Springer-Verlag, Berlin, Heidelberg, New York, 2003.

Abstract: Da una parte lo studio dei numeri, in particolare dei numeri primi, ha affascinato i matematici fin dalle epoche più antiche; d'altra parte, la sicurezza nella comunicazione dell'informazione è una necessità da sempre sentita dall'umanità. Negli ultimi vent'anni, grazie alla scoperta di nuovi metodi matematici e al notevole progresso nel campo dei computers, si è gradualmente sviluppato uno stretto rapporto tra le due discipline. Attualmente i metodi più sicuri per la trasmissione dell'informazione, che hanno recentemente avuto nuovo impulso dallo sviluppo del commercio elettronico, si basano su algoritmi che dipendono da notevoli proprietà dei numeri primi. In questo intervento tratteremo dapprima alcuni elementi dello sviluppo della teoria dei numeri primi; descriveremo poi un'applicazione al problema della sicurezza nella trasmissione dell'informazione, ossia alla crittografia.

- [13] A. Languasco, F. Menegazzo, and M. Morigi. On the composition length of finite primitive linear groups. *Arch. Math.*, 79:408–417, 2002. <http://dx.doi.org/10.1007/BF02638376>, MR1966776 (2004a:20051).

Abstract: Let G be a finite primitive linear group over a field K , where K is a finite field or a field of numbers. We bound the composition length of G in terms of the dimension of the underlying vector space and of the degree of K over its prime subfield. As a by-product, we prove a result of number theory which bounds the number of prime factors (counting multiplicities), of $q^n - 1$, where $q, n > 1$ are integers, improving a result of Turull and Zame.

- [14] A. Languasco and A. Perelli. Crittografia e firma digitale. In M. Emmer and M. Manaresi, editors, *Matematica, Arte, Tecnologia, Cinema*, pages 99–106, Bologna, 2002. Springer-Verlag, Milano. trad. inglese in *Mathematics, Art, Technology, and Cinema*, Springer-Verlag, Berlin, Heidelberg, New York, 2003.

Abstract: La sicurezza nella trasmissione dell'informazione è una necessità da sempre sentita dall'umanità. Nel corso dei secoli sono state utilizzate varie idee per questo scopo; esempi famosi sono il metodo di trasposizione di Giulio Cesare e la macchina di cifratura Enigma (utilizzata dalle forze armate tedesche durante la seconda guerra mondiale). I tentativi fatti precedentemente agli anni '70 non furono completamente soddisfacenti (si ricordi ad esempio la storia della forzatura del codice Enigma operata dal matematico A. Turing e dal suo gruppo negli anni '40); la possibilità di costruire un sistema crittografico rispondente a requisiti di sicurezza e autenticità fu provata a livello teorico da Diffie e Hellman nel 1976, mediante un rivoluzionario metodo detto a chiave pubblica. Tale idea trovò applicazione pratica due anni dopo, quando Rivest, Shamir e Adleman, utilizzando le proprietà dei numeri primi, concretizzarono l'idea di Diffie e Hellman. La crittografia moderna nasce quindi negli anni '70, e soppianta quasi completamente i metodi ottenuti come evoluzione delle idee classiche perché consente varie altre applicazioni. Ad esempio, la crittografia a chiave pubblica permette la costruzione di algoritmi efficienti e sicuri per l'autenticazione di documenti elettronici, ossia apre il campo ad una definizione di firma digitale.

- [15] A. Languasco. The exceptional set in short intervals for two additive problems with primes: a survey. *Riv. Mat. Univ. Parma (7)*, 3*:223–231, 2004. MR2128851 (2006a:11130).

Abstract: We give a brief account about the exceptional sets in short intervals for the Goldbach and the Hardy-Littlewood problems. In particular, we present two recent results about Montgomery-Vaughan's type estimates for such exceptional sets.

- [16] A. Languasco. On the exceptional set of Goldbach's problem in short intervals. *Monatsh. Math.*, 2004. <http://dx.doi.org/10.1007/s00605-003-0038-1>, MR2037990 (2004m:11162).

Abstract: Let E be the set of integers which are not a sum of two primes, $E(X) = E \cap [1, X]$ and $E(X, H) = E \cap [X, X + H]$, where $H = o(X)$. A well known result of Montgomery-Vaughan proves that there exists an absolute positive constant δ such that $|E(X)| \ll X^{1-\delta}$. Here we prove that there exists an absolute positive constant δ such that, for $H \geq X^{7/24+7\delta}$, $|E(X, H)| \ll H^{1-\delta/600}$, improving a result by Peneva.

- [17] A. Languasco. On the exceptional set for Hardy-Littlewood's numbers in short intervals. *Tsukuba J. Math.*, 28:169–192, 2004. <http://www.tulips.tsukuba.ac.jp/limedio/dlam/M73/M735867/11.pdf>, MR2082228 (2005d:11145). *Corrigendum ibid.*, *Tsukuba Journal of Mathematics*, **30** (2006), 237–240, MR2248294 (2007e:11124).

Abstract: In 1923 Hardy and Littlewood conjectured that every sufficiently large integer is either a k -power of an integer or a sum of a prime and a k -power of an integer, for $k = 2, 3$. We will call HL-numbers the integers that are a sum of a prime and a k -power of an integer. Let now $k \geq 2$ and denote by E_k the set of integers which are neither an HL-number nor a power of an integer. Here we prove that there exists an absolute positive constant δ such that for $H \geq X^{7/12(1-\frac{1}{k})+\delta}$

$$|E_k(X, H)| \ll H^{1-\delta/(5K)},$$

where $K = 2^{k-2}$, thus improving previous results by Perelli-Pintz, Mikawa, Perelli-Zaccagnini and Zaccagnini. In the Corrigendum we correct a mistake the treatment of the case $k = 2$.

- [18] A. Languasco. Primos Gemelos. *La Voz de Almeria, Seccion Matematica*, 2005. (pubblicato il 04/09/2005 in lingua spagnola, traduzione di Juan Cuadra Diaz).

Abstract: Breve articolo divulgativo riguardante la congettura dei primi gemelli.

- [19] A. Languasco and A. Zaccagnini. Alcune proprietà dei numeri primi, I. *Sito web Bocconi-Pristem*, 2005. <http://matematica-old.unibocconi.it/LangZac/home.htm>.

Abstract: È il primo di una serie di articoli divulgativi in cui si raccolgono proprietà dei numeri primi che di solito non si trovano nei libri di testo. In particolare, si parla del Teorema Fondamentale dell'Aritmetica, del Crivello di Eratostene e della densità dei primi nella successione dei numeri naturali. In Appendice si danno risultati più complessi.

- [20] A. Languasco and A. Zaccagnini. Alcune proprietà dei numeri primi, II. *Sito web Bocconi-Pristem*, 2005. <http://matematica-old.unibocconi.it/LangZac/home2.htm>.

Abstract: È il secondo di una serie di articoli divulgativi in cui si raccolgono proprietà dei numeri primi che di solito non si trovano nei libri di testo. Qui parliamo di criteri di primalità ed algoritmi di fattorizzazione, di certificati di primalità, di numeri primi di forma speciale. Anche qui, risultati più complessi sono dati in Appendice.

- [21] A. Languasco and A. Zaccagnini. Esistono piccoli intervalli fra primi consecutivi! *Sito web Bocconi-Pristem*, 2005. <http://matematica-old.unibocconi.it/LangZac/risultatoteorianumeri.htm>.

Abstract: Questo articolo è un breve annuncio per pubblicizzare un importante recente risultato di Goldston, Pintz e Yıldırım sull'esistenza di piccoli intervalli tra numeri primi consecutivi, ossia sul fatto che $\liminf(p_{n+1} - p_n) / \log p_n = 0$, dove p_n indica l' n -esimo numero primo.

- [22] A. Languasco and A. Zaccagnini. Intervalli fra primi consecutivi. *Sito web Bocconi-Pristem*, 2005. <http://matematica-old.unibocconi.it/LangZac/introduzione3.htm>.

Abstract: Questo articolo descrive lo stato dell'arte riguardo la questione degli intervalli fra numeri primi consecutivi, nei due casi di grandi o piccole deviazioni dal comportamento "medio." Dimostriamo alcuni risultati che, pur non essendo i migliori oggi noti, sono pur sempre non banali e illustrano bene le tecniche che si usano in questo campo. Questo articolo si rivolge a studenti universitari.

- [23] A. Languasco. On the sum of a prime and a k -free number. *Functiones et Approximatio, Commentarii Mathematici*, 34:19–26, 2006. <http://www.staff.amu.edu.pl/~fa/XXXIV/fa-34-1-019.pdf>, MR2269661 (2007j:11142).

Abstract: We prove an asymptotic formula (that refines old results by Walfisz and Mirsky) for the number of representations of sufficiently large integer as a sum of a prime and a k -free number, $k \geq 2$.

- [24] A. Languasco, J. Pintz, and A. Zaccagnini. On the sum of two primes and k powers of two. *Bull. London Math. Soc.*, 39:771–780, 2007. <http://dx.doi.org/10.1112/blms/bdm062>, MR2365226 (2008k:11107).

Abstract: Let X be a large integer. We prove that, for any fixed positive integer k , a suitable asymptotic formula for the number of representations of an even integer $N \in [1, X]$ as the sum of two primes and k powers of 2 holds with at most $\mathcal{O}_k(X^{3/5}(\log X)^{10})$ exceptions.

- [25] A. Languasco and A. Zaccagnini. A note on Mertens' formula for arithmetic progressions. *Journal of Number Theory*, 127:37–46, 2007. <http://dx.doi.org/10.1016/j.jnt.2006.12.015>, MR2351662 (2009g:11136).

Abstract: We study the Mertens product over primes in arithmetic progressions, and find a uniform version of previous results on the asymptotic formula, improving at the same time the size of the error term, and giving an alternative, simpler value for the constant appearing in the main term.

- [26] A. Languasco and A. Zaccagnini. On the Hardy-Littlewood problem in short intervals. *Int. J. Number Theory*, 4(5):715–723, 2008. <http://dx.doi.org/10.1142/S179304210800164X>, MR2458837 (2010a:11202).

Abstract: In this paper we will study the distribution of Hardy-Littlewood numbers in short intervals both unconditionally and conditionally, *i.e.* assuming the Riemann Hypothesis (RH). Our results concern the average of the asymptotic formula for the number of representations of an HL-number in almost all short intervals.

- [27] A. Languasco and A. Zaccagnini. Some estimates for the average of the error term of the Mertens product for arithmetic progressions. *Funct. Approx. Comment. Math.*, 38:41–47, 2008. <http://projecteuclid.org/euclid.facm/1229624650>, MR2433787 (2009f:11119).

Abstract: We give estimates for the error term of the Mertens product over primes in arithmetic progressions of the Bombieri–Vinogradov and Barban–Davenport–Halberstam type.

- [28] A. Languasco. A conditional result on the exceptional set for Hardy-Littlewood numbers in short intervals. *International Journal of Number Theory*, 5:9333–951, 2009. <http://dx.doi.org/10.1142/S179304210900247X>, MR2569737 (2010j:11146).

Abstract: Assuming the Generalized Riemann Hypothesis holds, we prove some conditional estimates on the exceptional set in short intervals for the Hardy-Littlewood problem.

- [29] A. Languasco and A. Zaccagnini. On the constant in the Mertens product for arithmetic progressions. II. Numerical values. *Math. Comp.*, 78:315–326, 2009. <http://dx.doi.org/10.1090/S0025-5718-08-02148-0>, MR2448709 (2010g:11164).

Abstract: We give explicit numerical values with 100 decimal digits for the constant in the Mertens product over primes in the arithmetic progressions $a \pmod q$, for $q \in \{3, \dots, 100\}$ and $(a, q) = 1$.

- [30] D. Bazzanella, A. Languasco, and A. Zaccagnini. Prime numbers in logarithmic intervals. *Trans. Amer. Math. Soc.*, 362(5):2667–2684, 2010. <http://dx.doi.org/10.1090/S0002-9947-09-05009-0>, MR2584615 (2011a:11171).

Abstract: Let X be a large parameter. We will first give a new estimate for the integral moments of primes in short intervals of the type $(p, p + h]$, where $p \leq X$ is a prime number and $h = o(X)$. Then we will apply this to prove that for every $\lambda > 1/2$ there exists a positive proportion of primes $p \leq X$ such that the interval $(p, p + \lambda \log X]$ contains at least a prime number. As a consequence we improve Cheer and Goldston's result on the size of real numbers $\lambda > 1$ with the property that there is a positive proportion of integers $m \leq X$ such that the interval $(m, m + \lambda \log X]$ contains no primes. We also prove other results concerning the moments of the gaps between consecutive primes and about the positive proportion of integers $m \leq X$ such that the interval $(m, m + \lambda \log X]$ contains at least a prime number. The last application of these techniques are two theorems (the first one unconditional and the second one in which we assume the validity of the Riemann Hypothesis and of a form of the Montgomery pair correlation conjecture) on the positive proportion of primes $p \leq X$ such that the interval $(p, p + \lambda \log X]$ contains no primes.

- [31] A. Languasco, A. Perelli, and A. Zaccagnini. On the Montgomery-Hooley theorem in short intervals. *Mathematika*, 52:231–243, 2010. <http://dx.doi.org/10.1112/S0025579310000628>, MR2678027 (2011g:11179).

Abstract: We study a short-interval version of a result due to Montgomery and Hooley. Write

$$S(x, h, Q) = \sum_{q \leq Q} \sum_{\substack{a=1 \\ (a,q)=1}}^q \left| \psi(x+h; q, a) - \psi(x; q, a) - \frac{h}{\varphi(q)} \right|^2$$

and $\kappa = 1 + \gamma + \log 2\pi + \sum_p (\log p)/p(p-1)$. Denote the expected main term by $M(x, h, Q) = hQ \log(xQ/h) + (x+h)Q \log(1+h/x) - \kappa hQ$. Let $\epsilon, A > 0$ be arbitrary, $x^{7/12+\epsilon} \leq h \leq x$ and $Q \leq h$. There exists a positive constant c_1 such that

$$S(x, h, Q) - M(x, h, Q) \ll h^{1/2} Q^{3/2} \exp\left(-c_1 \frac{(\log 2h/Q)^{3/5}}{(\log \log 3h/Q)^{1/5}}\right) + h^2 \log^{-A} x.$$

Now assume *GRH* and let $\epsilon > 0$, $x^{1/2+\epsilon} \leq h \leq x$ and $Q \leq h$. There exists a positive constant c_2 such that

$$S(x, h, Q) - M(x, h, Q) \ll \left(\frac{h}{Q}\right)^{1/4+\epsilon} Q^2 + hx^{1/2} \log^{c_2} x.$$

- [32] A. Languasco and A. Zaccagnini. Computing the Mertens and Meissel-Mertens constants for sums over arithmetic progressions. *Experimental Mathematics*, 19(3):279–284, 2010. With an appendix by Karl K. Norton. <http://www.informaworld.com/smp/content~db=all~content=a933386262~frm=titlelink>, MR2743571 (2011j:11247).

Abstract: We give explicit numerical values with 100 decimal digits for the Mertens constant involved in the asymptotic formula for $\sum_{\substack{p \leq x \\ p \equiv a \pmod{q}}} 1/p$ and, as a by-product, for the Meissel-Mertens constant defined as $\sum_{p \equiv a \pmod{q}} (\log(1 - 1/p) + 1/p)$, for $q \in \{3, \dots, 100\}$ and $(q, a) = 1$. The complete set of results can be downloaded from the webpage: <http://www.math.unipd.it/~languasc/Mertens-comput.html>

- [33] A. Languasco and A. Zaccagnini. On a Diophantine problem with two primes and s powers of two. *Acta Arith.*, 145:193–208, 2010. <http://journals.impan.gov.pl/cgi-bin/aa/pdf?aa145-2-07>, MR2733083 (2011i:11046).

Abstract: We refine a recent result of Parsell on the values of the form $\lambda_1 p_1 + \lambda_2 p_2 + \mu_1 2^{m_1} + \dots + \mu_s 2^{m_s}$, where p_1, p_2 are prime numbers, m_1, \dots, m_s are positive integers, λ_1/λ_2 is negative and irrational and $\lambda_1/\mu_1, \lambda_2/\mu_2 \in \mathbb{Q}$.

- [34] A. Languasco and A. Zaccagnini. On the constant in the Mertens product for arithmetic progressions. I. Identities. *Functiones et Approximatio, Commentarii Mathematici*, 42(1):17–27, 2010. <http://projecteuclid.org/euclid.facm/1269437065>, MR2640766 (2011b:11127).

Abstract: We give new identities for the constants in the Mertens product over primes in the arithmetic progressions $a \pmod{q}$, extending previous work by Uchiyama, Grosswald, Williams and Moree.

- [35] A. Languasco and V. Settimi. On a Diophantine problem with one prime, two squares of primes and s powers of two. *preprint, to appear in Acta Arithmetica*, 2012. <http://arxiv.org/abs/1103.1985>.

Abstract: We refine a result of W.P. Li and Wang on the values of the form $\lambda_1 p_1 + \lambda_2 p_2^2 + \lambda_3 p_3^2 + \mu_1 2^{m_1} + \dots + \mu_s 2^{m_s}$, where p_1, p_2, p_3 are prime numbers, m_1, \dots, m_s are positive integers, $\lambda_1, \lambda_2, \lambda_3$ are nonzero real numbers, not all of the same sign, λ_2/λ_3 is irrational and $\lambda_i/\mu_i \in \mathbb{Q}$, for $i \in \{1, 2, 3\}$.

- [36] A. Languasco and A. Zaccagnini. The number of Goldbach representations of an integer. *Proc. Amer. Math. Soc.*, 140:795–804, 2012. <http://dx.doi.org/10.1090/S0002-9939-2011-10957-2>.

Abstract: Let Λ be the von Mangoldt function and $R(n) = \sum_{h+k=n} \Lambda(h)\Lambda(k)$ be the counting function for the Goldbach numbers. Let $N \geq 2$ and assume that the Riemann Hypothesis holds. We prove that

$$\sum_{n=1}^N R(n) = \frac{N^2}{2} - 2 \sum_{\rho} \frac{N^{\rho+1}}{\rho(\rho+1)} + \mathcal{O}(N \log^3 N),$$

where $\rho = 1/2 + i\gamma$ runs over the non-trivial zeros of the Riemann Zeta-function $\zeta(s)$. This improves a recent result by Bhowmik and Schlage-Puchta.

- [37] A. Languasco and A. Zaccagnini. Sums of many primes. *Journal of Number Theory*, 132:1265–1283, 2012. <http://dx.doi.org/10.1016/j.jnt.2011.11.004>.

Abstract: Assuming that the Generalized Riemann Hypothesis (GRH) holds, we prove an explicit formula for the number of representations of an integer as a sum of $k \geq 5$ primes. Our error terms in such a formula improve by some logarithmic factors an analogous result by Friedlander-Goldston.

- [38] A. Languasco, A. Perelli, and A. Zaccagnini. Explicit relations between pair correlation of zeros and primes in short intervals. to appear in *Journal of Mathematical Analysis and Applications*, 2012.

Abstract: In this paper we obtain a quantitative version of the celebrated theorem by D.A. Goldston and H.L. Montgomery about the equivalence between the asymptotic behaviors of the mean-square of primes in short intervals and of the pair-correlation function of the zeros of the Riemann zeta function.

- [39] A. Languasco and A. Zaccagnini. A Diophantine problem with a prime and three squares of primes. submitted, 2012.

Abstract: We refine a recent result of Li-Wang on the values of the form $\lambda_1 p_1 + \lambda_2 p_2^2 + \lambda_3 p_3^2 + \lambda_4 p_4^2$, where p_1, p_2, p_3, p_4 are prime numbers, $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ are nonzero real numbers, not all of the same sign, and λ_1/λ_2 is irrational.

- [40] A. Languasco and A. Zaccagnini. L^2 -norms of exponential sums over prime powers. submitted, 2012.

Abstract: We study a suitable mean-square average of primes in short intervals, generalizing Saffari-Vaughan's result. We then apply it to a ternary Diophantine problem with prime variables.

- [41] A. Languasco and A. Zaccagnini. A Diophantine problem with prime variables. submitted, 2012.

Abstract: We study the distribution of the values of the form $\lambda_1 p_1 + \lambda_2 p_2 + \lambda_3 p_3^k$, where λ_1, λ_2 and λ_3 are non-zero real number not all of the same sign, with λ_1/λ_2 irrational, and p_1, p_2 and p_3 are prime numbers. We prove that, when $1 < k < 4/3$, these value approximate rather closely any prescribed real number.

- [42] A. Languasco and A. Zaccagnini. *Crittografia*. CLEUP, Padova, 2006. Progetto Lauree Scientifiche per il Veneto.

Abstract: Queste sono le note del materiale preparato per lo svolgimento degli Incontri del Progetto Nazionale Lauree Scientifiche per il Veneto, sottoprogetto Matematica, per la tematica Crittografia.

- [43] A. Languasco and A. Zaccagnini. *Introduzione alla Crittografia*. Ulrico Hoepli Editore, 2004.

Abstract: Lo scopo primario degli autori è la presentazione del linguaggio della Crittografia moderna e dei suoi problemi. Il libro fornisce la base matematica che permette di comprenderne il funzionamento, al fine di consentire un utilizzo più consapevole degli strumenti crittografici anche a chi non ha intenzione di diventare un professionista del campo. Vengono presentati alcuni sistemi crittografici simmetrici (DES, AES) ed asimmetrici (fra i quali il popolare RSA), la cui sicurezza è basata sulla presunta difficoltà dei problemi della fattorizzazione dei numeri interi e del logaritmo discreto. In particolare sono analizzati gli attacchi noti a RSA ed alcune precauzioni implementative, sono trattati gli algoritmi necessari per implementare i crittosistemi e sono descritti alcuni Protocolli crittografici utilizzati al giorno d'oggi. Inoltre è introdotto uno strumento specifico per calcoli teorico-numeric (PARI/GP). Arricchiscono questo volume numerosi esempi, diagrammi e figure che lo rendono accessibile a qualunque lettore.

Prof. Alessandro Languasco, Ph. D.
Indirizzo Dipartimento di Matematica, via Trieste 63, 35121 Padova
Telefono 049 8271385
Fax 049 8271479
e-mail languasco@math.unipd.it
pagina web <http://www.math.unipd.it/~languasc>

